CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

AI AND CYBERSECURITY LAW: PROTECTING AGAINST AI-POWERED CYBER THREATS

Aishwarya Singh[1*]
[1*]Research Scholar, Banasthali Vidyapith

***Corresponding Author:** Aishwarya Singh*
**Research Scholar, Banasthali Vidyapith*

ABSTRACT
This paper's objectives are to evaluate the applicability of current international instruments to combat cybercrime in light of artificial intelligence (AI) technologies and to offer a brief overview of ongoing international organizations' policy initiatives that could soon have a significant influence on the development of cybercrime legislation. This essay addresses the implications that developing AI policies might have for managing the criminal justice system, particularly with regard to combating cybercrimes. Deep fakes and other contemporary developments in the usage of AI apps and systems to carry out destructive and unlawful actions are examined. The report concludes with a suggestion for a different approach to developing efficient policy solutions to stop cybercrime using AI systems.
Over the last decade, cyber threats have become a challenge for the proficient. Current security systems need more advancement to deal with exceptionally trained cybercriminals. Implementing Artificial Intelligence (AI) techniques helps detect scams but may bring other risks. This research paper focuses on the intersection between cyber security threats and their forestallment using Artificial Intelligence (AI) technologies. It briefly outlines Artificial Intelligence (AI) applications for several cybersecurity crimes and estimates the probability of expanding cybersecurity by conservation of the defense mechanisms. The innovation of Artificial Intelligence has unlocked new room for the world's future. The methods to secure data have influenced the growth of Artificial Intelligence (AI) in cybersecurity.
The paper aims to establish awareness regarding the benefits of Artificial Intelligence (AI) technology and
its assistance in protecting on a larger scale, i.e., in an organization or a business. The statistics mentioned
in the paper are taken from valid sources and proved to favor the study.
This study assesses the potential for increasing cybersecurity capabilities by strengthening the defensive mechanism and offers a succinct summary of artificial intelligence (AI) implementations of various cybersecurity employing artificial technologies. After reviewing the state-of-the-art artificial intelligence cybersecurity software, we may deduce that useful applications already exist. First and foremost, they deploy neural networks to safeguard several other cybersecurity domains as well as the peripheral. However, it was evident that the effective resolution of some cybersecurity issues would need the application of artificial intelligence techniques. For instance, detailed information is crucial for making strategic decisions, and one of the unresolved cybersecurity challenges is the need for logical decision support.

KEYWORD: Artificial Intelligence, Cyber Security, Cyber Attack, Machine Learning, AI Surveillance,

INTRODUCTION
Artificial Intelligence (AI) is a rapidly expanding field. In the next ten years, AI technology is expected

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

to be widely accessible in homes, offices, businesses, and the general public. It will permeate nearly every aspect of our lives. There is a global shift occurring in the way governments and the public use AI technology for security. Flying to any major airport in the world or passing through the central business district of any large city has been all that has been necessary in the previous ten years to discover AI monitoring in action.

These days, artificial intelligence (AI) permeates many of the items we consider "smart" in our homes, including phones, smart watches, drones, self-driving cars, robotic vacuums and lawnmowers, and drones. Artificial intelligence (AI) is widely used in robotics, technology, the medical field (particularly in diagnosis and surgery), transportation, the military, video games, government and public administration, insurance, finance and economics, auditing, advertising, and the arts, among many other fields. Furthermore, it has been progressively incorporated into the legal sphere, encompassing predictive justice and court outcome prediction.

"Cyberlaw" or information technology law is the legal term for laws relating to information technology, which includes computers and the internet. It is in charge of managing information security, electronic commerce, and the digital dissemination of software and information. It has a connection to legal informatics. It's also known as "paper laws" for a "paperless environment" according to some. In addition to intellectual property in computing and the internet, it raises specific issues with contract law, privacy, freedom of expression, and jurisdiction. IT law, which is not a separate area of law in and of itself, includes legislation pertaining to data protection, contracts, intellectual property, and privacy. Intellectual property comprises copyright, fair use policies, copy protection policies tailored to digital media, and workarounds for these policies. It is significant part of law.

Regulations control the flow of information between private companies and the general public, as well as the harmony between censorship and freedom of speech. Laws define what data can be collected and retained for law enforcement needs and what data cannot be collected for privacy reasons. In certain circumstances and legal jurisdictions, computer communications may be used as evidence and to generate contracts. The guidelines that regulate the use of modern computer-enabled methods of surveillance and tapping differ substantially in terms of what law enforcement can and cannot present in court as evidence. A variety of legal issues are raised by computerized voting technologies, such as those used at polling places, websites, and smartphones. Some states impose legal and technical restrictions on Internet access.

CYBER LAWS IN INDIA:

Any technology-based crime in India that involves the use of a computer as a tool for cybercrime is prohibited by cyber laws. Cybercrime laws protect people from giving personal information to strangers they don't know online. The IT Act 2000, introduced and amended in 2008, has covered a variety of categories of offences from the inception of cyber laws in India. The Act lists the many types of cybercrimes and their associated punishments.

By definition, cyber law is a subset of law that addresses problems pertaining to internet technology. Cyber law in India pertains specifically to offences committed through the use of a computer or other electronic device. The legislation pertaining to information technology, which includes computers and the internet, is known as cyber law, often known as IT law? It oversees software, e-commerce, information security, and the digital exchange of information. It is associated with legal informatics. IT law encompasses elements of contract, intellectual property, privacy, and data protection laws rather than being a distinct field of law. One important component of IT law is intellectual property. In Europe and other places, the contentious field of software licensing is still developing.[1]

[1] GeeksforGeeks, "Cyber law (IT Laws) In India", retrieved from

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

According to the Ministry of Electronics and Information Technology, Government of India: Cyber Laws yields legal recognition to electronic documents and a structure to promote e-filing and e-commerce transactions and also provides a legal structure to minimize.
There are several importance of Cyber Security which are as discussed below:-

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include[2]:

1. **Fraud:** Cyber laws are what shield consumers from online fraud. Legislation is created to stop online financial crimes such as credit card theft, identity theft, and others. Identity theft offenders may be charged with state or federal felonies. They may also run into a victim-brought civil case. Cyber attorneys fight accusations of online fraud as well as prosecute cases involving such charges.
2. **Copyright:** Copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.
3. **Defamation:** Many employees express their opinions online. It can become defamatory when someone use the internet to spread false information. Defamation laws are civil rules that protect people from making false claims in public that could damage someone's reputation or a company. When someone uses the internet to say things that are illegal under civil law, this is known as defamation law.
4. **Harassment and Stalking:** Sometimes, comments made online are regarded as crimes that forbid harassment and stalking. When someone makes threats against another person on the internet, it is against both criminal and civil law. Cyber attorneys prosecute and defend stalker victims by using the internet and other electronic communication means.
5. **Freedom of Speech:** One key aspect of cyber law is freedom of speech. Freedom of speech rules permit people to express their opinions even when cyber laws prohibit specific online behaviors. Cyber attorneys are required to counsel their clients with the boundaries of free speech, especially laws that forbid profanity. When there is a disagreement about whether their conduct qualify as acceptable free speech, cyber attorneys may also defend their clients.
6. **Contract and Employment Laws:** Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

ARTIFICIAL INTELLEGENCE (AI):

The focus of artificial intelligence (AI) has been on how robots behave or reason in specific situations. This common term includes the degree to which robots are capable of thought or behavior similar to that of humans. It's a way to find out if a computer is behaving human-like. When a human being conversing with a computer is unable to discern whether the responses are coming from the computer or from the human, the computer is considered intelligent.

---

https://www.geeksforgeeks.org/cyber-laws-in-india/ visited on 17 July 2024.
[2] *Supra* Note 1

CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

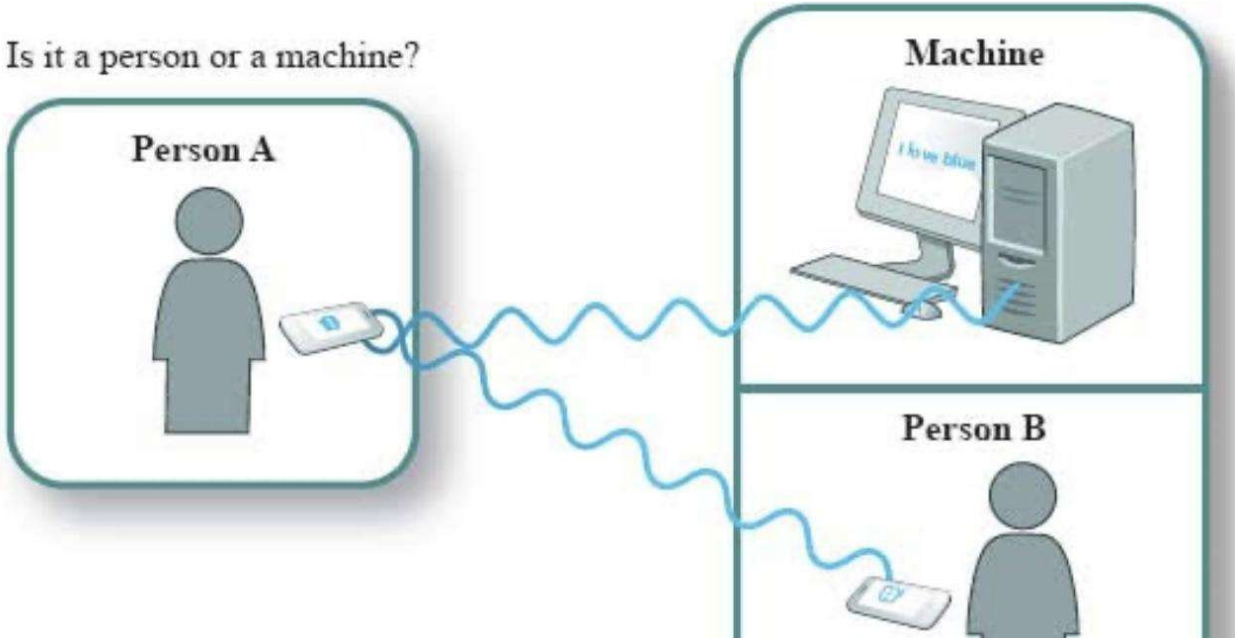


FIGURE 1. Turing test in Artificial Intelligence (AI)

Intrusion detection systems (IDS) are the most relevant application of artificial intelligence (AI) technology in the context of cyber threats. A software programme called an intrusion detection system (IDS) searches a network for hostile activity or strategy infractions. The system usually reports any breach centrally. A large amount of internet traffic may be analyzed and categorised by artificial intelligence (AI).
Cybersecurity solutions based on Machine Learning (ML) technologies are used to automate the recognition of attacks and to improve their capabilities. Machine Learning (ML) solutions are used in intrusion detection systems (IDS). Machine learning (ML) techniques learn from the collected internet traffic to discriminate the malicious from the legitimate traffic class. It is the method of detecting malware networks and phishing emails. It uses algorithms and requires human intervention to correct errors.[3]

Machine learning: Conventionally, machine learning (ML) approaches can be classified into two groups: supervised and unsupervised learning. Supervised machine learning studies the relationship between labeled input and output training data. The samples are labeled according to their class (e.g., malicious or legitimate). In unsupervised machine learning, no data labeling or training is required. The nomenclature perspectives are converging, making it less essential to define machine learning algorithms based on whether they are supervised or unsupervised.[4]

[3] Rajashree Manjulalayam Rajendran, Bhuman Vyas, "Cyber Security Threat And Its Prevention Through Artificial Intelligence Technology" *International Journal for Multidisciplinary Research (IJFMR)* E-ISSN: 2582-2160, 2023
[4] Ibid

CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

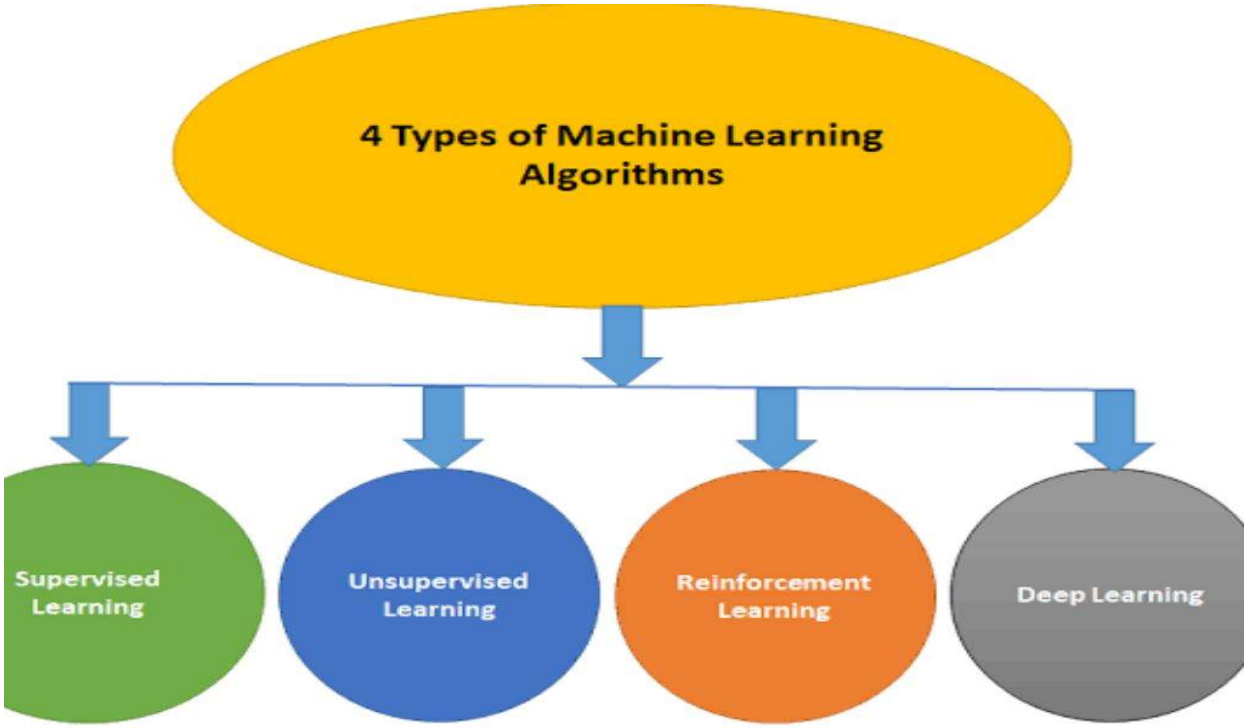


FIGURE 5. Machine Learning (Supervised & unsupervised)

AI IN DEPTH:

Artificial intelligence (AI) is a relatively new field of research, having existed for almost as long as computer systems (also known as first system intelligence). AI was "on the horizon" in the early years when it was thought that machines, software, and structures would be created that were smarter than people. The problem is that the time frame is getting longer as time goes on. We witnessed a range of machines, for instance, mastering chess and solving logically challenging puzzles.[5]

In the early stages of the computing, chess play was considered an intellectual test. Even though electronic chess was on the rise in the 1970s, it seemed nearly impossible to create a system that could beat the world champion. But this happened faster than expected. Three factors account for this: enhanced computing capacity and the creation of potent search algorithms. Beyond games like chess, it could be used in a variety of software applications, such as skill sets that are well-organized and contain all conceivable chess knowledge. Since the chess problem was an abstract worry of the so-called tiny AI, it was essentially resolved. Another instance pertains to the translation of a certain AI from one dialect to another.[6]

The 1960s are expected to tackle the problem of natural language processing early on, particularly in

[5] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). "Building a multiagent environment for military decision support tools with semantic services". *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* 6070 LNAI (PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7_19 visited on 1 June 2024.

[6] Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). "Innovations in Hybrid Intelligent Systems" *Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems* (HAIS'07). 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1 visited on 1 June 2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

the wake of N. Chomski's computational linguistics research. Though some innovative programmes, like Google's AI linguistics, showed early promise, it hasn't happened yet. This includes artificial intelligence becoming extremely knowledgeable about every facet of human activity and developing the ability to handle it. In general, artificial intelligence (AI) can be understood as a component of intellect and, more broadly, as the development of intelligent devices. AI is a technology that provides a way to solve complex problems that cannot be solved by, say, performing well or making wise decisions because of high levels of intelligence.[7]

ROLE OF AI IN CYBER SECURITY

Does AI represent cybersecurity's future? Businesses in the public and private sectors have already embraced AI initiatives, and as the White House points out, numerous federal agencies also make use of the technology. Why? Why? AI is capable of saving a lot of time and resources by skimming through standardized data and thoroughly examining unstructured data, numbers, voice patterns, and words. Actually, AI has the potential to protect national secrets as well as tax cash. There are also gaps. Hackers are attempting to discover ways to get inside the devices by finding gaps in security that we were unaware of. Years pass before a business discovers a data leak. By then, all of the sensitive data has vanished along with the hacker.

Conversely, AI has to wait till a hacker gets dirty and just gather data. AI looks for a variety of behavioral irregularities that hackers might exhibit, such as when a user logs in or when a password is written. Artificial intelligence (AI) is able to identify subtle indicators that a hacker group would have missed otherwise and halt them in their tracks. Like Varughese pointed out, anything may be misused. In the ongoing cybersecurity chess game, human hackers will always probe the weak points in any system, including artificial intelligence. Because artificial intelligence is controlled by humans, it can still be defeated. Artificial intelligence (AI) can only work as intended, despite its amazing ability to link and interpret data.[8] Programmers will need to implement new defenses as hackers adapt to Artificial Intelligence systems. The cat and mouse game will continue, but artificial intelligence is a useful ally in the struggle to protect data. For Tensor Flow machine learning, Google unveiled a graphical data learning approach. Search results for March 9, 2019 implemented Neural Structured Learning (NSL), an open-source framework for training data sets and data structures in neural nets using the Neural Graph Learning technique. NSL is intended for qualified machine learning specialists in addition to those who lack expertise, and it integrates with the Tensor Flow stage of machine learning. NSL can run NLP, render machine vision models, and project data from interactive databases, including information graphs and medical records.

The connection between artificial intelligence and cybersecurity one important component that influences computer decision-making is artificial intelligence. For example, the computer may detect unusual behaviour on the system and refuse access unless the relevant authority grants permission. These artificial intelligence techniques leverage machine learning, a process whereby computer scientists develop algorithms using data gathered over time. Because of the way the algorithm is constructed, it can recognize and discern between authentic and fraudulent access. Machine learning technology improves an organization's security by making threats and anomalies more predictable.[9] The

[7] Feyereisl, J., & Aickelin, U. (2009). S Elf -O Rganising M Aps. August, 1–30.

[8] Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). "An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system". *IEEE Transactions on Fuzzy Systems*, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616. Visited on 1 June 2024

[9] Ibid

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

precision and speed with which threats are identified are unmatched by humans. As a consequence, artificial intelligence and machine learning technologies can avert cyber-attacks that might cost your company millions. Nevertheless, businesses must continue to update security systems as hackers evolve in response to technological advancements

BENEFITS OF AI IN CYBER SECURITY

AI has become a powerful tool in the fight against cyber threats as it can help detect, analyze, and respond to malicious attacks faster. Leveraging AI helps you better understand your networks and identify potential threats faster. AI-powered solutions can sift through vast amounts of data to identify abnormal behavior and detect malicious activity, such as a new zero-day attack. AI can also automate many security processes, such as patch management, making staying on top of your cyber security needs easier. It can help you respond faster to attacks by automating specific tasks, such as rerouting traffic away from a vulnerable server or alerting your IT team to potential issues.

When it comes to accuracy and efficiency, AI-based cyber security systems outperform conventional security solutions. For instance, in a fraction of the time it would take human operators to perform the same operation, AI can scan a vast number of devices for potential vulnerabilities. Additionally, patterns that can be hard for the human eye to see can be recognized by AI systems, improving the accuracy of harmful activity identification. By automating time-consuming security chores, AI can free up precious resources to concentrate on other business areas.

It is also faster than a human at identifying risks because it can handle enormous amounts of data reliably and rapidly. This lowers the cost of protecting against cyber threats and speeds up the response time to security issues. By connecting disparate data sources, AI-driven solutions can also assist in identifying harmful activities, giving you the ability to safeguard your systems proactively. Since these solutions are readily scalable, you can add more security without having to shell out a lot of money for hardware or staff.

The Risk of Relying on AI in Cyber Security

Businesses all around the world are significantly investing in AI because of its unequalled security against cyber-attacks and its capacity to analyses enormous data sets quickly. However, there are still hazards associated with depending on AI, even as its use in enhancing security grows. AI systems that make biased decisions may come from a variety of sources, such as algorithms that lack the requisite objectivity or data sets that contain biased information. Improper management of these biases can result in discriminatory judgments made against specific groups or individuals, which can have major ramifications for the organisation.

For example, a decision made by an AI system based on biased inputs could lead to false positives and block legitimate users from accessing company systems, resulting in lost productivity or customers. The algorithms used to make decisions about security threats are not always transparent, leaving you vulnerable to potential bias or manipulation. AI can be difficult to interpret, so it's hard to understand why decisions were made or how they can be improved.

This lack of understanding can lead to poor decisions, which can have severe implications for an organization's security. AI-based cyber security solutions may not always accurately identify every threat or potential breach, leading to potential risks going unnoticed and causing further damage. AI algorithms can be designed to search through data and detect patterns quickly, making them an attractive target for malicious actors who could use them to access sensitive information or attack infrastructure.

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

Examples of AI in Cyber Security-

Cyber criminals may use AI to:

- Easily create new malware that can contain new zero-day vulnerabilities or bypass detection.
- Create new, sophisticated, original, or targeted phishing attacks. Such actions can increase the number of scenarios, making it difficult for reputation engines to keep up.
- Analyze and collect data much quicker and help identify other avenues of attack.
- Create (video or audio) that can be used to convince victims in social engineering attacks.
- Conduct attacks such as intrusions or generate new hacking tools.

And because AI relies on data sets that are often biased or incomplete, it can lead to missed threats and false positives, creating a false sense of security and leading to real-world consequences.

CONCLUSION

The impact of artificial intelligence on cybersecurity and threat mitigation was assessed in this study. The results imply that advances in technology have made it easier for hackers to improve the strategies, techniques, and tools they employ to exploit individuals and institutions. Artificial intelligence can be detrimental even though it has many positive uses. Making informed technological decisions will help organisations avoid a calamity. Artificial intelligence (AI) is rapidly emerging as a vital instrument for enhancing information security organizations' efficacy. Artificial intelligence (AI) offers the much-needed monitoring and threat detection that security experts can use to lessen the likelihood of a breach and strengthen their organization's defence capabilities. Humans are no longer able to adequately secure an enterprise level attack surface.

Furthermore, artificial intelligence may assist in the discovery and prioritization of risks, the direction of incident response, and the identification of malware cyber-attacks before they occur. As a result, even with the possible drawbacks, artificial intelligence will aid to advance cybersecurity and assist businesses in developing a stronger overall security.

Reference

1. S.G Akojwar, P Kshirsagar-2016 "A Novel Probabilistic-PSO Based Learning Algorithm for Optimization of Neural Networks for Benchmark Problems"- WSEAS TRANSACTIONS on ELECTRONICS, Volume 7, 2016.
2. P. Kshirsagar and S. Akojwar, "Classification & Detection of Neurological Disorders using ICA & AR as Feature Extractor", Int. J. Ser. Eng. Sci. IJSES, vol. 1, no. 1, Jan. 2015.
3. Pravin Kshirsagar, Sudhir Akojwar & Nidhi Bajaj(2020),"A hybridised neural network and optimisation algorithms for prediction and classication of neurological disorders", International Journal of Biomedical Engineering and Technology Volume 28, Issue 4 ,DOI: 10.1504/IJBET.2018.095981
4. P. Kshirsagar and S. Akojwar, "Novel approach for classification and prediction of non- linear chaotic databases," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 514-518, doi: 10.1109/ICEEOT.2016.7755667.
5. P. R. Kshirsagar, H. Manoharan, F. Al-Turjman, and K. Kumar, Design and testing of automated smoke monitoring sensors in vehicles," IEEE Sensors Journal, vol. 1, p. 1, 2020.

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

6. H. Manoharan, Y. Teekaraman, P. R. Kshirsagar, S. Sundaramurthy, and A. Manoharan, "Examining the effect of aquaculture using sensor-based technology with machine learning algorithm," Aquaculture Research, vol. 51, no.11, pp. 4748–4758, 2020.
7. Golda Dilip, Ramakrishna Guttula, Sivaram Rajeyyagari, Hemalatha S, Radha Raman Pandey, Ashim Bora, Pravin R Kshirsagar, Khanapurkar M M, Venkatesa Prabhu Sundramurthy, "Artificial Intelligence-Based Smart Comrade Robot for Elders Healthcare with Strait Rescue System", Journal of Healthcare Engineering, vol. 2022, Article ID 9904870, 12 pages, 2022. https://doi.org/10.1155/2022/9904870.
8. Kshirsagar, P. R., Chippalkatti, P. P., & Karve, S. M. (2018). Performance optimization of neural network using GA incorporated PSO. Journal of Advanced Research in Dynamical and Control Systems, 10(4).
9. Kshirsagar, P., & Akojwar, S. (2016). Prediction of neurological disorders using optimized neural network. In International conference on signal processing, communication, power and embedded system (SCOPES).
10. Kshirsagar, P., & Akojwar, S. (2016). Optimization of BPNN parameters using PSO for EEG signals. In Proceedings of the international conference on communication and signal processing, 2016 (ICCASP 2016).
11. Kshirsagar, P., & Akojwar, S. (2016). Hybrid heuristic optimization for benchmark datasets. International Journal of Computer Applications, 146(7), 11–16.
12. Kshirsagar, P., & Akojwar, S. (2015). Classification and prediction of epilepsy using FFBPNN with PSO. In IEEE international conference on communication networks.
13. Kshirsagar, P., Balakrishnan, N., & Yadav, A. D. (2020). Modelling of optimised neural network for classification and prediction of benchmark datasets. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 8(4), 426–435.
14. Akojwar, S., Kshirsagar, P., & Pai, V. (2014). Feature extraction of EEG signals using wavelet and principal component analysis. National Conference on Research Trends in Electronics, Computer Science & Information Technology and Doctoral Research Meet, Feb 21st &22nd
15. Pravin Kshirsagar et.al (2016), "Brain Tumor classification and Detection using Neural Network", DOI: 10.13140/RG.2.2.26169.72805.
16. Pravin Kshirsagar and Sudhir Akojwar (2017), "Classification of ECG-signals using Artificial Neural Networks", Researchgate.net
17. Pravin Kshirsagar and Sudhir Akojwar (2016) "Classification of Human Emotions using EEG Signals" International Journal of Computer Applications (0975 – 8887) Volume 146 – No.7, July 2016.

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

18. Pravin Kshirsagar and Sudhir Akojwar(2015), “Classification and Prediction of Epilepsy using FFBPNN with PSO”, IEEE International Conference on Communication Networks, 2015.
19. Alterazi HA, Kshirsagar PR, Manoharan H, Selvarajan S, Alhebaishi N, Srivastava G, Lin JC-W. Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. Sensors. 2022; 22(16):6117. https://doi.org/10.3390/s22166117. Swagat M. Karve.et.al / REST Journal on Emerging trends in Modelling and Manufacturing, 8(2) 2022, 99-106 Copyright@ REST Publisher
103
20. Shitharth, S.; Prasad, K.M.; Sangeetha, K.; Kshirsagar, P.R.; Babu, T.S.; Alhelou, H.H. An Enriched RPCO-BCNN Mechanisms for Attack Detection and Classification in SCADA Systems. IEEE Access 2021, 9, 156297–156312
21. Shitharth, S.; Prasad, K.M.; Sangeetha, K.; Kshirsagar, P.R.; Babu, T.S.; Alhelou, H.H. An Enriched RPCO BCNN Mechanisms for Attack Detection and Classification in SCADA Systems. IEEE Access 2021, 9, 156297–156312
22. Akojwar, S.; Kshirsagar, P. A Novel Probabilistic-PSO Based Learning Algorithm for Optimization of Neural Networks for Benchmark Problems. Wseas Trans. Electron. 2016, 7, 79–84.
23. Kshirsagar, Pravin R., Hariprasath Manoharan, Shitharth Selvarajan, Sara A. Althubiti, Fayadh Alenezi, Gautam Srivastava, and Jerry Chun-Wei Lin. 2022. "A Radical Safety Measure for Identifying Environmental Changes Using Machine Learning Algorithms" Electronics 11, no. 13: 1950. https://doi.org/10.3390/electronics11131950
24. Sundaramurthy, S.; Saravanabhavan, C.; Kshirsagar, P. Prediction and Classification of Rheumatoid Arthritis using Ensemble Machine Learning Approaches. In Proceedings of the 2020 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, 8–9 November 2020; pp. 17–21.
25. S. Oza, “IoT: the future for quality of services,” in Proceedings of the ICCCE 2019, A. Kumar and S. Mozar, Eds., vol. 570, Springer, Singapore, December 2019, Lecture Notes in Electrical Engineering.
26. P. Kshirsgar, V. More, V. Hendre, P. Chippalkatti, and K. Paliwal, “IOT based baby incubator for clinic,” in Proceedings of the ICCCE 2019, A. Kumar and S. Mozar, Eds., vol. 570, Springer, Singapore, August 2020, Lecture Notes in Electrical Engineering
27. Pravin R. Kshirsagar, Hariprasath Manoharan, Samir Kasim, Asif Irshad Khan, Md Mottahir Alam, Yoosef B. Abushark, Worku Abera, "Expedite Quantification of Landslides Using Wireless Sensors and Artificial Intelligence for Data Controlling Practices", Computational

ISSN:1624-1940
DOI 10.6084/m9.figshare.2631024
http://magellanes.com/

Intelligence and Neuroscience, vol. 2022, Article ID 3211512, 11 pages, 2022. https://doi.org/10.1155/2022/3211512.

28. Kshirsgar P., More V., Hendre V., Chippalkatti P., Paliwal K. (2020) IOT Based Baby Incubator for Clinic. In: Kumar A., Mozar S. (eds) ICCCE 2019. Lecture Notes in Electrical Engineering, vol 570. Springer, Singapore.

https://doi.org/10.1007/978-981-13-8715-9_42.

29. Kshirsgar P., More V., Hendre V., Chippalkatti P., Paliwal K. (2020) IOT Based Baby Incubator for Clinic. In: Kumar A., Mozar S. (eds) ICCCE 2019. Lecture Notes in Electrical Engineering, vol 570. Springer, Singapore.

https://doi.org/10.1007/978-981-13-8715-9_42

30. Shitharth, S.; Meshram, P.; Kshirsagar, P.R.; Manoharan, H.; Tirth, V.; Sundramurthy, V.P. Impact of Big Data Analysis on Nanosensors for Applied Sciences using Neural Networks. J. Nanomater. 2021, 2021, 4927607
31. V. Velvizhi, S.R. Billewar, G. Londhe, P. Kshirsagar, N. Kumar Big data for time series and trend analysis of poly waste management in India Mater. Today:. Proc., 37 (Part 2) (2021), pp. 2607-2611, 10.1016/j.matpr.2020.08.507,2021
32. Hariprasath Manoharan, Radha Krishna Rambola, Pravin R. Kshirsagar, Prasun Chakrabarti, Jarallah Alqahtani, Quadri Noorulhasan Naveed, Saiful Islam, Walelign Dinku Mekuriyaw, "Aerial Separation and Receiver Arrangements on Identifying Lung Syndromes Using the Artificial Neural Network", Computational Intelligence and Neuroscience, vol. 2022, Article ID 7298903, 8 pages, 2022. https://doi.org/10.1155/2022/7298903
33. G. Dilip, R. Guttula, S. Rajeyyagari et al., "Artificial intelligence-based smart comrade robot for elders healthcare with strait rescue system," Journal of Healthcare Engineering, vol. 2022, Article ID 9904870, 12 pages, 2022.
34. Kshirsagar, Pravin&Manoharan, and Hariprasath, "An operational collection strategy for monitoring smart waste management system using shortest path algorithm," Journal of Environmental Protection and Ecology, vol. 22, pp. 566–577, 2021.
35. P. Kshirsagar, "Brain Tumor Classification and Detection Using Neural Network," in Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 83–88, IEEE, Tiruchengode, India, January, 2020
36. Nabeel Albishry, Rayed AlGhamdi, Abdulmohsen Almalawi, Asif Irshad Khan, Pravin R. Kshirsagar, undefined BaruDebtera, "An Attribute Extraction for Automated Malware Attack Classification and Detection Using Soft Computing Techniques", Computational International.